UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,895	01/16/2004	Guy Eden	SLA1496	8472

7590   11/13/2007

Law Office of Gerald Maliszewski
P.O. Box 270829
San Diego, CA 92198-2829

EXAMINER
SAN JUAN, MARTINJERIKO P

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/759,895	EDEN ET AL.
	Examiner	**Art Unit**	
	Martin Jeriko P. San Juan	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 September 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-10,13-27,30,31 and 34</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-10,13-27,30,31 and 34</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>29 May 2007</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 08-06)   Office Action Summary   Part of Paper No./Mail Date 20071029

DETAILED ACTION

This is a response to Applicant's Amendments and Remarks filed on September 27, 2007. Claims 1-34 were pending. Claims 1-5, 13-20, 27, 30-31, and 34 have been amended. Claims 11-12, 28-29, and 32-33 have been cancelled. Claims 1-10, 13-27, 30-31, and 34 are currently pending.

Response to Arguments

1.   Applicant's arguments filed on September 27, 2007 have been fully considered but they are not persuasive.

Applicant respectfully submits that a prima facie case of obviousness has not been supported in the rejections. With regard to the Applicant's invention, the Applicant argues that the amended claims limit a user to a particular resource corresponding to a particular key. This means that each printer resource is associated with a particular key (K), so that a print job can be sent with information unlock just one specific printer resource. The combination of references fails to disclose a secure means of delivering a combination of encrypted hash and encrypted encryption key that limits access to just one particular resource, for one particular print job. Therefore, the combination for

references does not teach every limitation associated with claims 1, 17, 18, and

34.

The Examiner respectfully disagrees by asserting that a prima facie case of

obviousness has been established. The rejections under 35 USC 103(a) under

Morgan et al. [US 5220674], Wiegley [US 6711677], and Konsella et al. [US

6856317] are being maintained while incorporating the amended claims and

further explanation behind the rejections. Most or all suggestions/motivations are

in the references themselves. There is a reasonable expectation of success

because it has been explained clearly how a person ordinary skill in the art at the

time of invention would have combined these references. And even though the

individual reference themselves may not teach all the claim limitations, the

references when combined as shown and explained do teach or suggest all the

claim limitations. Refer to the claim rejections explained in section of Claim

Rejection under 35 USC 103.

Applicant further argues that Wiegley discloses a two-way communication

process where link security is established in response to sending a session

identifier to the node originating the print job, receiving a session identifier back

in a reply, and comparing the received session identifier with the originally-sent

identifier. In contrast, the claimed invention uses a one-way link between nodes

– the claimed invention first device does not send a session identifier. Another

general difference is that Wiegley's process is designed to protect a print job

being transmitted from one node to another. The claimed invention is designed

to securely access a resource that is already stored in the memory of the

destination node. Further Wiegley does not disclose the processing of the print

job using the decrypted resource. And with regard to Konsella, Konsella does

not disclose a secure means of transmitting or delivering a decryption key to a

printer. Konsella does not even disclose a means of associating encryption keys

with particular secured resources.

Examiner respectfully reminds the Applicant that while the individual reference

themselves may not teach all the claim limitations, the references when

combined as shown and explained do teach or suggest all the claim limitations.

Refer to the rejections and explanations in section of Claim Rejection under 35

USC 103. With regard to "Konsella not disclosing a means of associating

encryption keys with particular secured resources," the Examiner respectfully

disagrees and points that it would have been inherent because of the evidence

that encryption/decryption keys exist for particular resources as cited in the in the

section of Claim Rejection under 35 USC 103.

Claim Objections

1.   Claim 10 is objected to because of the following informalities:

a.   It appears that claim 10 should have been amended to incorporate the

amendments of claim 1. Though it appears it has been amended, it has not been

declared. For the purpose of examination, the Examiner is still maintaining the

previous rejection because the subject matter being claimed would have been

the same as the previous one.

Appropriate correction is required.

2.   Claims 13-14 and 16 objected to because of the following informalities:

b. N_i must be corrected to N_k, since N_i is not defined.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness

under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.

2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

1.   Claims 1-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Morgan et al. [US PN 5220674], and further in view of Wiegley [US PN 6711677 B1]

and Konsella et al. [US PN 6856317 B2].

Regarding Claim 1, Morgan et al. teaches a method for network-connected resources,

the method comprising: at a first network-connected node, receiving an <u>unencrypted</u>

electronically formatted job [US PN 5220674, Col 6, Ln 55-58], receiving a selection

command for a particular one of a plurality of resources [US 5220674, Col 4, Ln 13-21 –

Examiner notes that it is inherent that a selection command for a particular one of a

plurality of resources is received from a particular printing request if the resource

manager has knowledge for supplying the needed resource from the plurality of

resources stored as evidenced by the cited passage.] and using a resource to process

the job [US PN 5220674, Col 7, Ln 24-29].

Morgan et al. does not teach receiving CK, a symmetrical encryption key (K) encrypted

using an asymmetrical encryption public key (pubK); receiving CH, a hash (H) of the

job, further encrypted using K; decrypting CK using an asymmetrical encryption private

key (privK), corresponding to pubK, to recover K; hashing the job, generating H'; using

K to validate CH.

Weigley teaches a secure printing method comprising: receiving CK [session key – US PN 6711677 B1, Col 4, Ln 49], a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK) [encrypted session key with printer public key – US PN 6711677 B1, Col 4, Ln 54]; receiving CH, a hash (H) of the job, further encrypted using K [compute hash value for print data, encrypt hash value using session key – US PN 6711677 B1, Col 5, Ln 32]; decrypting CK using an asymmetrical encryption private key (privK), corresponding to pubK, to recover K [printer decrypts session key using its private key – US PN 6711677 B1, Col 5, Ln 4]; hashing the job, generating H' [printer computes hash value of print data -- US PN 6711677 B1, Col 5, Ln 36]; using K to validate CH [US PN 6711677 B1, Col 5, Ln 36-39];

It would have been obvious to one of ordinary skill in the art at the time of invention to add cryptographic security as taught by Weigley in the method of using network-connected resources of Morgan et al. because there is no security precautions in the method of Morgan et al. The suggestion/motivation for combining would have been to provide security to the access and use of network-connected resources by validating the print job [US PN 6711677 B1, Col 2, Ln 35-53] that would essentially access and use the resource. Morgan et al. and Weigley are analogous art because they are both in the same field of endeavor involving printing systems. Therefore, it would have been obvious to combine the inventions of Morgan et al. and Weigley.

Konsella et al. teaches a system and method for storing public and secure font data in a

font file which is a form of printing resources comprising: receiving a selection

command for a particular one of a plurality of resources [US 6856317 B2, Col 5, Ln 3-

15]; in response to a validation of use, decrypting an encrypted resource using a

decryption key [US PN 6856317 B2, Col 4, Ln 44-56]; and also providing a particular

decryption key corresponds to a particular encrypted resource [US 6856317 B2, Col 5,

Ln 11] [US 6856317 B2, Col 6, Ln 17-20].

It would have been obvious to one of ordinary skill in the art at the time of invention to

add cryptographic security as taught by Konsella et al. in the actual use of network-

connected resources of Morgan et al. because these secure font files can be stored

easily in the printer server's internal collection of resources. The suggestion/motivation

for combining would have been to provide security to the use of network-connected

resources such as fonts and glyphs [US PN 6856317 B2, Col 2, Ln 1-50] and for ease

of maintaining these secured resources [US PN 6856317 B2, Col 5, Ln 30-40]. Morgan

et al. and Konsella et al. are analogous art because they are both in the same field of

endeavor involving printing systems that also solves the problem of security. Therefore

it would have been obvious to combine the inventions of Morgan et al. and Konsella et

al.

Since both Morgan and Konsella teach receiving a selection command for a particular

one of a plurality of resources, and Konsella alone teaches providing a particular

decryption key that corresponds to a particular encrypted resource [US 6856317 B2,

Col 6, Ln 17-20], it follows that Morgan combined with Konsella would suggest that a

particular printing request would comprise a particular decryption key corresponding to

a particular encrypted resource such that it would have been taught wherein receiving a

selection command for a particular one of a plurality of encrypted resources includes

receiving K^r_i, where $1 \leq i \leq m$, where K^r_i is the decryption key taught by Konsella [US

6856317 B2, Col 5, Ln 11]. Also, the fact that decryption and encryption keys are used

interchangeably by Konsella [US 6856317 B2, Col 5, Ln 6-12] to enable the encrypted

printer resource would have suggested that such a cryptographic key would have been

a symmetrical key.

However, Morgan and Konsella by themselves do not teach K^r_i being encrypted using

an asymmetrical encryption public key (pubK). As such, the combined invention of

Morgan and Konsella do not teach wherein receiving a selection command for a

particular one of a plurality of encrypted resources includes receiving CK_i, where $1 \leq i \leq$

m; and wherein decrypting the selected resource in response to the encrypted resource

selection command includes decrypting CK_i to recover one of symmetrical encryption

keys K_1 through K_m, where K_1 through K_m correspond to encrypted resources CR_1

through CR_m.

Weigley teaches that it is common and well known in the art to provide security in the

exchange of a key between two nodes in a network known as dual key systems [US PN

6711677 B1, Col 1, Ln 19-26]. As such, Weigley uses the dual key systems to teach

receiving a cryptographic key CK [session key – US PN 6711677 B1, Col 4, Ln 49],

which is a symmetrical encryption key (K) encrypted using an asymmetrical encryption

public key (pubK) [encrypted session key with printer public key – US PN 6711677 B1,

Col 4, Ln 54]; decrypting a cryptographic key CK, using an asymmetrical encryption

private key (privK), corresponding to pubK, to recover K [printer decrypts session key

using its private key – US PN 6711677 B1, Col 5, Ln 4].

The invention of Morgan and Konsella combined with Weigley would have taught that

K^r_i of Konsella be encrypted using an asymmetrical encryption public key such that

receiving a selection command for a particular one of a plurality of encrypted resources

includes receiving CK^r_i, where $1 \leq i \leq m$.

Furthermore, the invention of Morgan and Konsella combined with Weigley would have

taught that K^r_i of Konsella be encrypted using an asymmetrical encryption public key

such that decrypting the selected resource in response to the encrypted resource

selection command includes decrypting CK^r_i to recover one of symmetrical encryption

keys K^r_1 through K^r_m, where K^r_1 through K^r_m correspond to encrypted resources CR_1

through CR_m.

Also it would have been obvious to one of ordinary skill in the art at the time of invention

to use Konsella's symmetric key of protecting the printer resource to be directly related

to the key data of Weigley's symmetrical key of protecting the transmission of the print

job because the print job being requested is directly tied to the needed printer resource

as taught by Morgan [US 5220674, Col 4, Ln 13-21] such that combining Morgan,

Wiegley, and Konsella would have taught CK^r_i to be CK_i.

The suggestion/motivation for combining all three references would have been to

provide security of a confidential print job [US 6711677 B1, Col 1, Ln 50-57]. Since a

print job is tied directly to the access of a network connected printer resource, it follows

another suggestion/motivation for combining which is to provide security to the access

and use of a network-connected resources by validating the print job [US PN 6711677

B1, Col 2, Ln 35-53] that would essentially access and use the resource. Providing

security to the actual use of the network-connected resources such as fonts and glyphs

[US PN 6856317 B2, Col 2, Ln 1-50] and for the ease of maintaining these secured

resources [US PN 6856317 B2, Col 5, Ln 30-40] are another suggestion/motivation for

the references to be combined. Lastly, providing security in the transmission/exchange

of cryptographic keys is already known in the art as dual keys systems [US PN 6711677

B1, Col 1, Ln 19-26] which would have been another suggestion/motivation to combine.

Morgan, Wiegley, and Konsella are analogous art because they are all in the same field

of endeavor involving printing systems. Each reference also solves each other's

problems/deficiencies concerning security issues as explained in the above

suggestions/motivations. Therefore, it would have been obvious to combine Morgan, Wiegley, and Konsella.

Regarding claim 2, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 1 using K_i to validate CH_i as follows:

encrypting H' using K_i, obtaining CH_i'; and, matching CH_i to CH_i' [US PN 6711677 B1, Col 5, Ln 36-39 -- This method claim is an obvious variant of claim 3. H is inherent in CH using the symmetrical key, K.].

Regarding claim 3, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 1 using K_i to validate CH_i as follows: decrypting CH_i using K_i, generating H; and, comparing H to H' [US PN 6711677 B1, Col 5, Ln 36-39].

Regarding claim 4, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 1 further comprising: prior to receiving the job, CK_i, and CH_i, receiving the encrypted resource; and storing the encrypted resource [US 6856317 B2, Col 5, Ln 36].

Regarding claim 5, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 4 further comprising: installing pubK and privK upon initialization [US PN 6711677 B1, Col 4, Ln 31-34].

Regarding claim 6, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 1 wherein receiving the unencrypted electronically formatted job includes receiving a print job in a format selected from the group including text and image formats [US PN 5220674, Col 6, Ln 58-61].

Regarding claim 7, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 4 wherein storing the encrypted resource includes storing an encrypted font resource [US PN 6856317 B2, Col 5, Ln 32-36]; and wherein using the decrypted resource to process the job includes printing a print job using the decrypted fonts [US PN 6856317 B2, Col 5, Ln 5-6].

Regarding claim 8, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 7 wherein storing the encrypted font resource includes storing resources selected from the group including a logo, personal signature image, and glyph [US PN 6856317 B2, Col 2, Ln 54-62].

Regarding claim 9, the combined inventions of Morgan et al., Wiegley, and Konsella et al. teaches the method of claim 4 wherein receiving the encrypted resource includes receiving the encrypted resource in a format selected from the group including hypertext transport protocol (http) and file transport protocol (FTP) [US PN 6856317 B2, Col 5, Ln 30-40 -- Konsella et al. teaches distributing secure font data files including emailing to recipients which implies an internet network connection. HTTP and FTP are standard

internet protocols for communicating data in the internet, as such, these protocols are
inherent.].

Regarding claim 10, the combined inventions of Morgan et al., Wiegley, and Konsella et
al. teaches the method of claim 1 further comprising: at a second network-connected
node, generating the job [US PN 5220674, Col 6, Ln 55-58]; encrypting K with pubK,
generating CK [encrypted session key with printer public key – US PN 6711677 B1, Col
4, Ln 54]; hashing the job, generating H [US PN 6711677 B1, Col 5, Ln 32]; encrypting
H using K, generating CH [US PN 6711677 B1, Col 5, Ln 32]; and, sending the job, CK,
and CH to the first node for job processing [US PN 6711677 B1, Col 5, Ln 32-34].

Regarding claim 13, the combined inventions of Morgan, Wiegley, and Konsella teaches
the method of claim 1 wherein receiving the unencrvpted electronically formatted job
includes receiving the job at network-connected node N_k, where $1 \leq k \leq n$; wherein
receiving CK includes N_i receiving CK_{ik}, where CK_{ik} is generated by encrypting K_i using
corresponding asymmetrical encryption public key $pubK_k$; and, wherein decrypting CK
includes N_i decrypting CK_{ik} using corresponding asymmetrical encryption private key
$privK_k$, to recover K_i. [This is rejected based on obviousness directed on implementing
a plurality of the combined invention of Morgan, Wiegley, and Konsella of claim 1.]

Regarding claim 14, the combined inventions of Morgan, Wiegley, and Konsella teaches
the method of claim 1 wherein receiving the unencrvpted electronically formatted job

includes receiving the job at network-connected node N_k, where $1 \leq k \leq n$; wherein receiving CK includes N_i receiving CK_{ik}, corresponding to symmetrical encryption key K_{ik}, encrypted using $pubK_k$; wherein receiving CH includes N_i receiving CH_{ik}, a hash of the job encrypted using corresponding symmetrical encryption key K_{ik}; and wherein decrypting CK includes N_i decrypting CK_{ik} using asymmetrical encryption private key $privK_{ik}$, to recover corresponding symmetrical encryption key K_{ik}. [This is rejected based on obviousness directed on implementing a plurality of the combined invention of Morgan, Wiegley, and Konsella of claim 1.]

Claim 15 has the same limitations as claim 2 with the accommodation of the plurality of the invention in claim 1. Claim 15 is rejected based on obviousness and using the same references and rationale of claim 2.

Claim 16 has the same limitations as claim 3 with the accommodation of the plurality of the invention in claim 1. Claim 16 is rejected based on obviousness and using the same references and rationale of claim 3.

Claim 17 is rejected because it is still directed to the same invention of claim 1.

Claim 18 is rejected using the same references as claim 1. Claim 18 is merely a system performing the methods of claim 1.

Claims 19-27 and 30-31 are rejected using the same references and rationale claims 2-

10, and 13-14 respectively because it is the system performing the methods of claims 2-

10, and 13-14.

Claim 34 is rejected using the same reference and rationale as claim 17 which is still

directed to the same invention of claim 1.

Conclusion

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Martin Jeriko P. San Juan whose telephone number is

571-272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Also, **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

/MJSJ/

Martin Jeriko San Juan

Examiner. Art Unit 2132

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100